RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: LAB3-W01

Translating Threats into Deception Strategies

Diego Staino
R&D+i Manager
BASE4 Security
/in/diegostaino/

Federico Pacheco
Cybersecurity Services Director
BASE4 Security
/in/federicopacheco/

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

About us

Diego Staino
R&D+i Manager
14+ years of consulting experience
Bachelor in Information Security

Federico Pacheco
Cybersecurity Services Director
20+ years of university teaching experience
4 published books | 15+ whitepapers

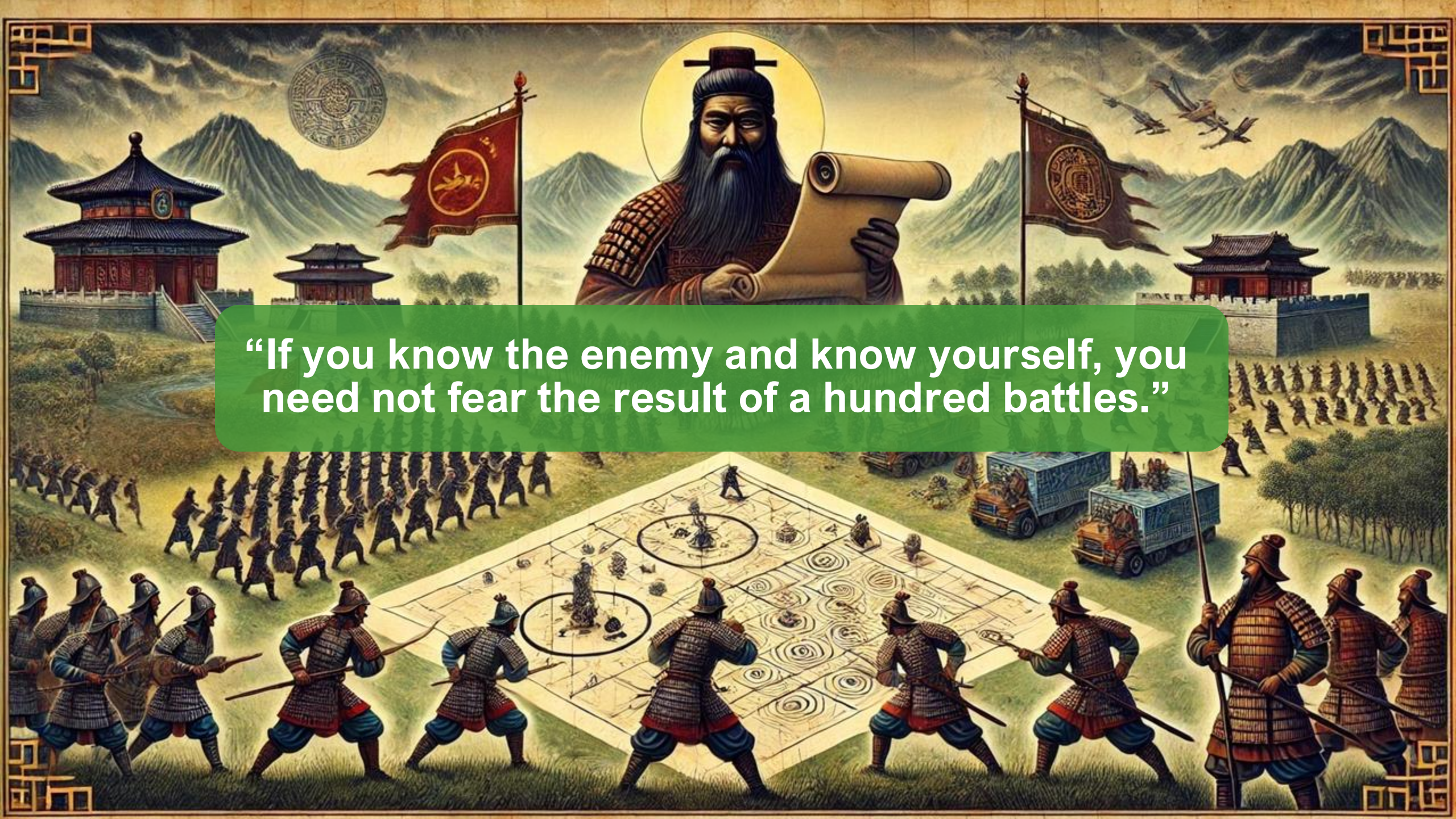
Learning Lab Agenda

- Cyber Deception 101
- Phase 1 - Behavior Extraction
- Phase 2 - Criteria Selection
- Phase 3 - Translation of TTPs into activities
- Phase 4 - Storytelling Design
- Q&A and Wrap-Up

RSAC 2025 Conference

Cyber Deception 101

“In times of deception, telling the truth is a revolutionary act”


“If you know the enemy and know yourself, you need not fear the result of a hundred battles.”

Intro to Deception

* with offensive approach

* +detect or hinder

"A **defensive** practice designed to deceive attackers by setting **traps** and **decoys** in an infrastructure or system that mimic real-world assets."

*or they are real

*our

512 BC

MITRE | Engage™

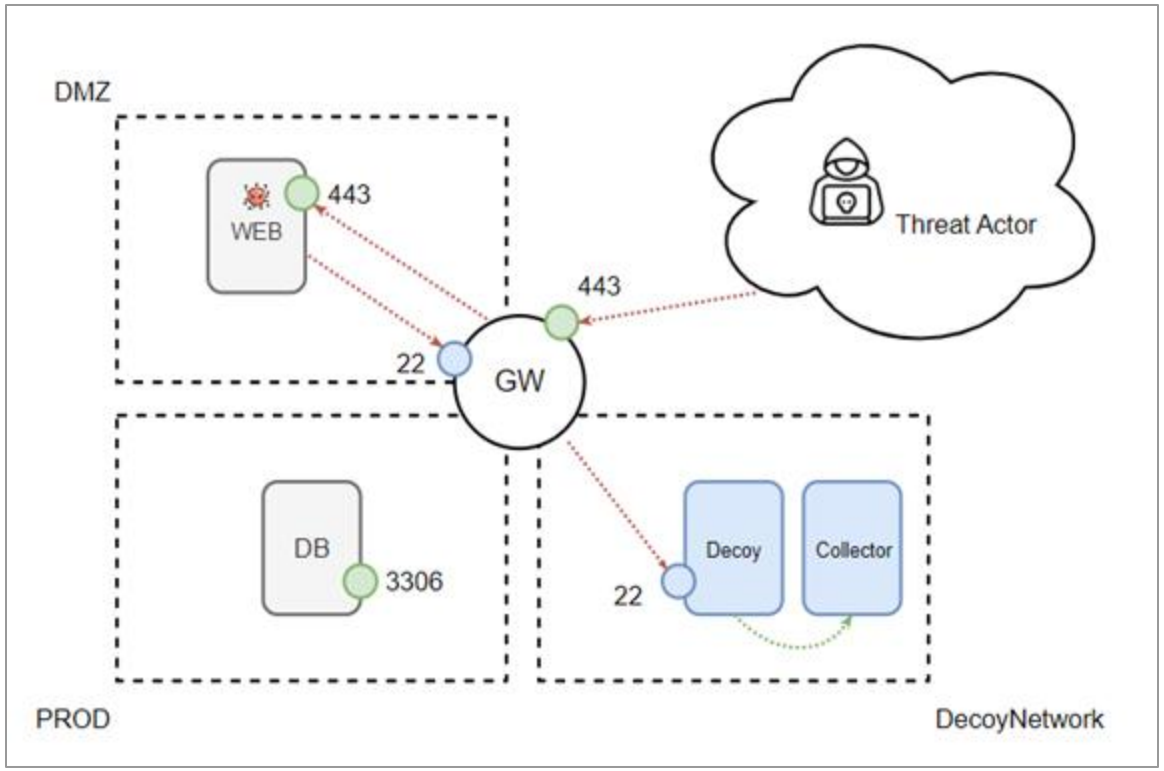
2022

TTPs and Threat Intelligence

MITRE ATT&CK™

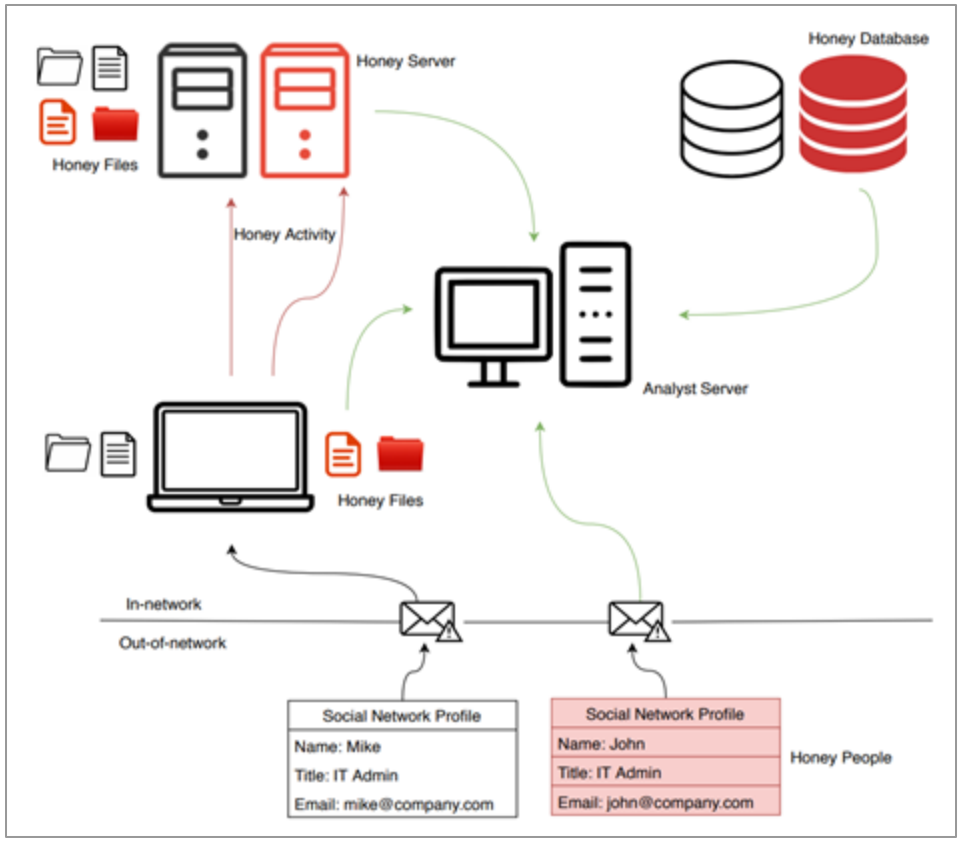
What types of cyber deception activities are you aware of?
(2 minutes)

Let's see some cases



DOLOS Tool - Use Case for Web Server

Paper: "Proposal for the implementation of minimalistic cyber deception strategies" Pacheco, Staino, 2024



Paper: "Detecting Targeted Attacks By Multilayer Deception" Wang et al, 2013

RSAC 2025 Conference

Behavior Extraction

“We don’t see things as they are, we see them as WE are”

What about TTPs?

"XXX leverage DNS tunneling for data exfiltration"

"YYY use PowerShell to execute scripts"

"ZZZ use print processors to run malicious DLLs"

Indicator ≠ IoC ≠ Behavioral invariant ≠ TTP

Tools and methodologies

Log & Trace analysis

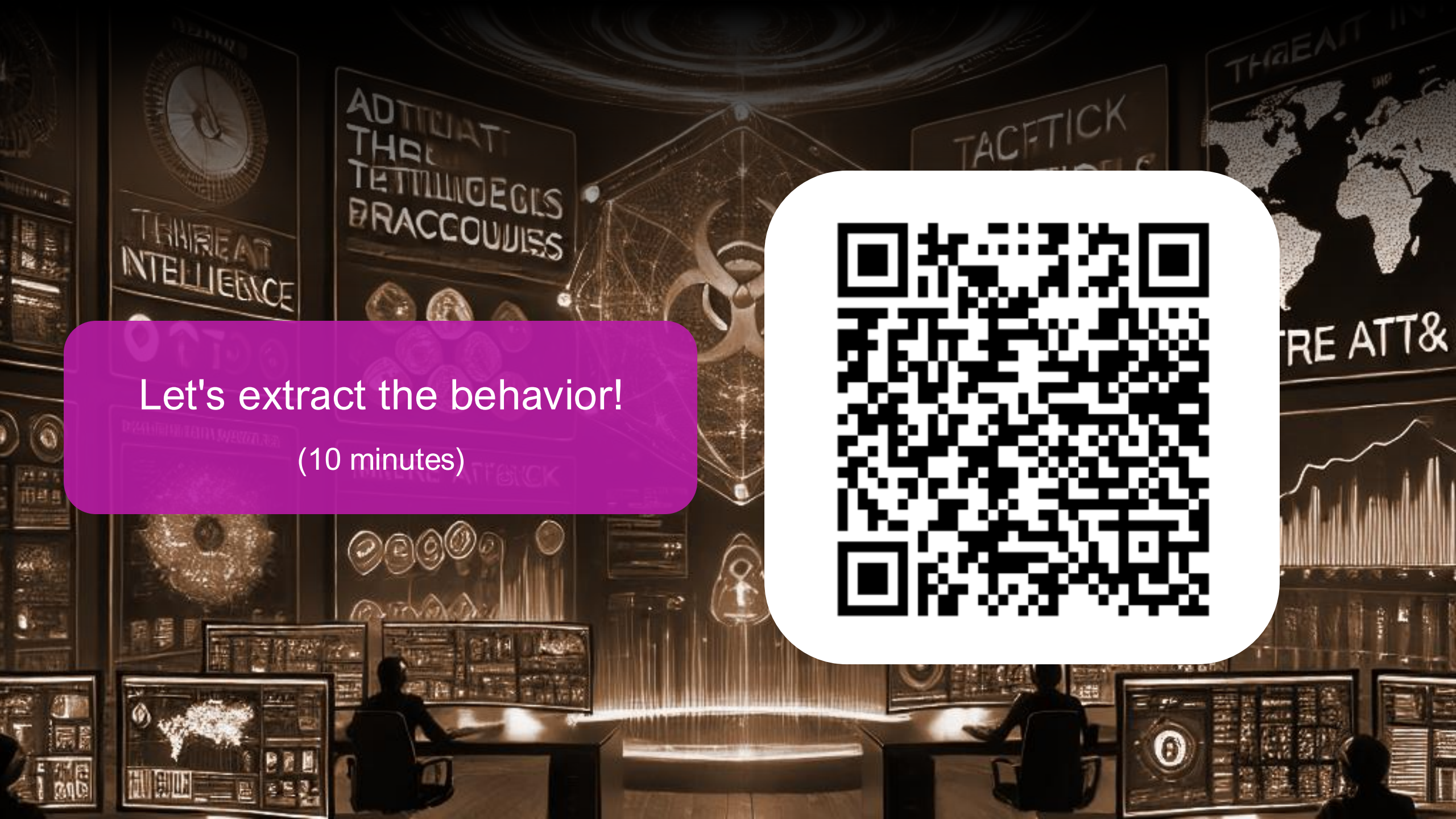
- Data correlation
- Sandboxing
- Look for Interesting activity

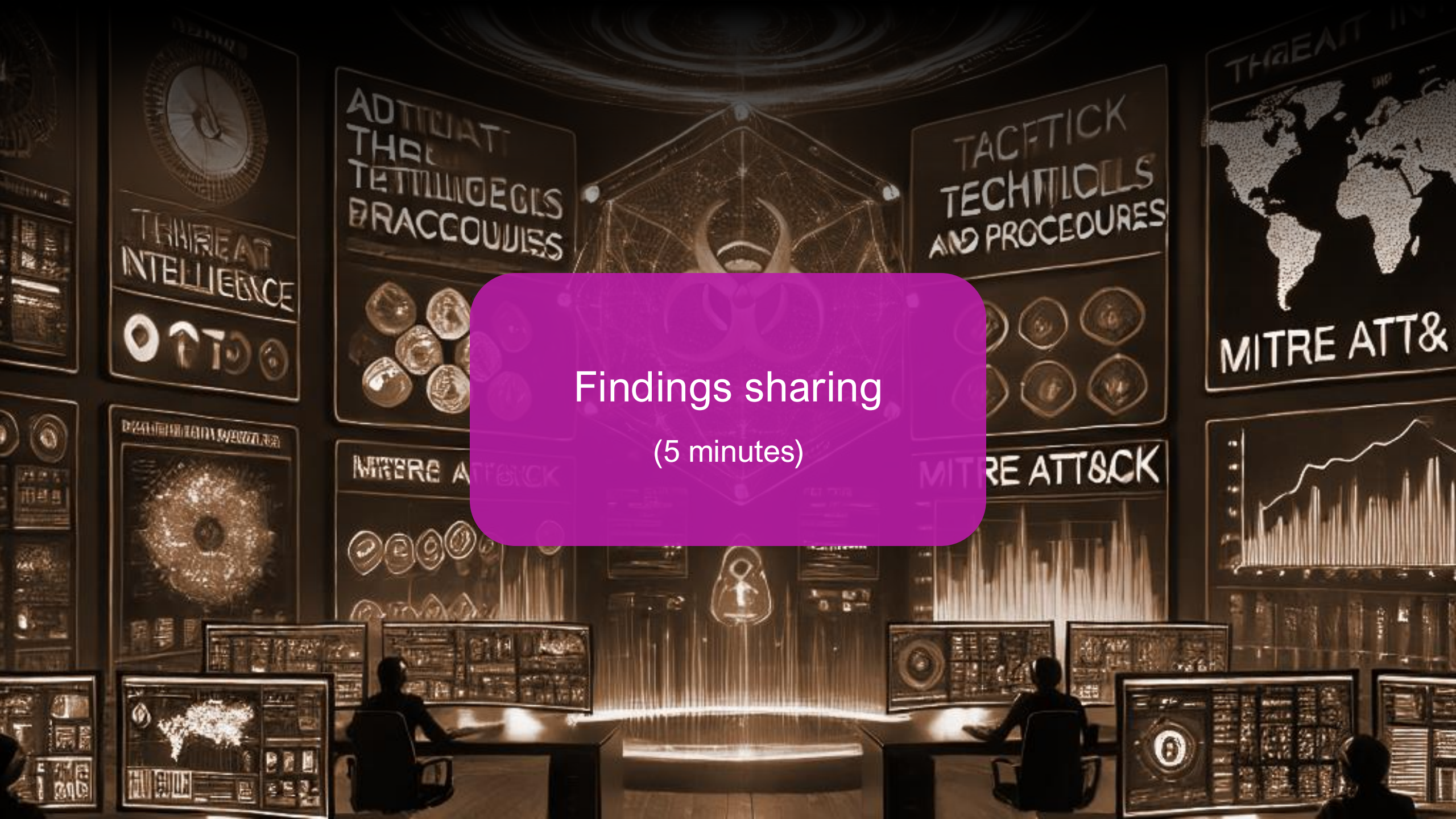
OSINT & CTI Platforms

- OpenCTI | Maltego | Dark Web
- VirusTotal | MISP

Reports from Govs & Orgs

MITRE ATT&CK | CISA | Europol EC3
FIRST | Mandiant | CrowdStrike
SentinelOne | Unit 42


Let's extract the behavior!
(10 minutes)

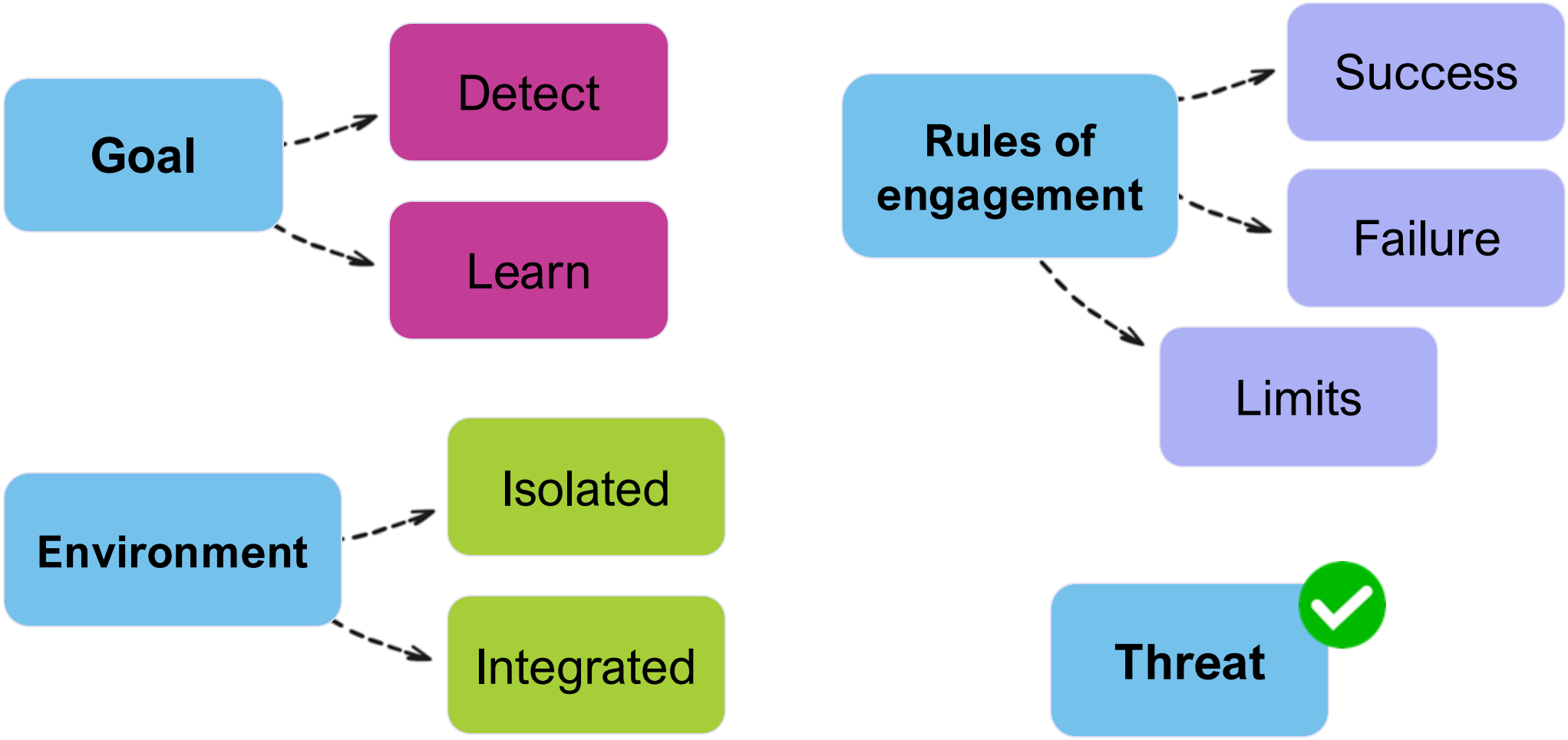

Findings sharing
(5 minutes)

RSAC 2025 Conference

Criteria Selection

“A well-chosen lie is like a tailor-made suit: it fits perfectly for the occasion, even if it’s not made of truth.”

Base element selection



Understanding Risk & Impact

What if …

… the adversary uses your env to distribute malware?

… a decoy user is detected using a prod service?

… a zero-day is exploited in the isolated env?

* Release your anxiety and ask questions *

Establishing criteria for the operation

(10 minutes)

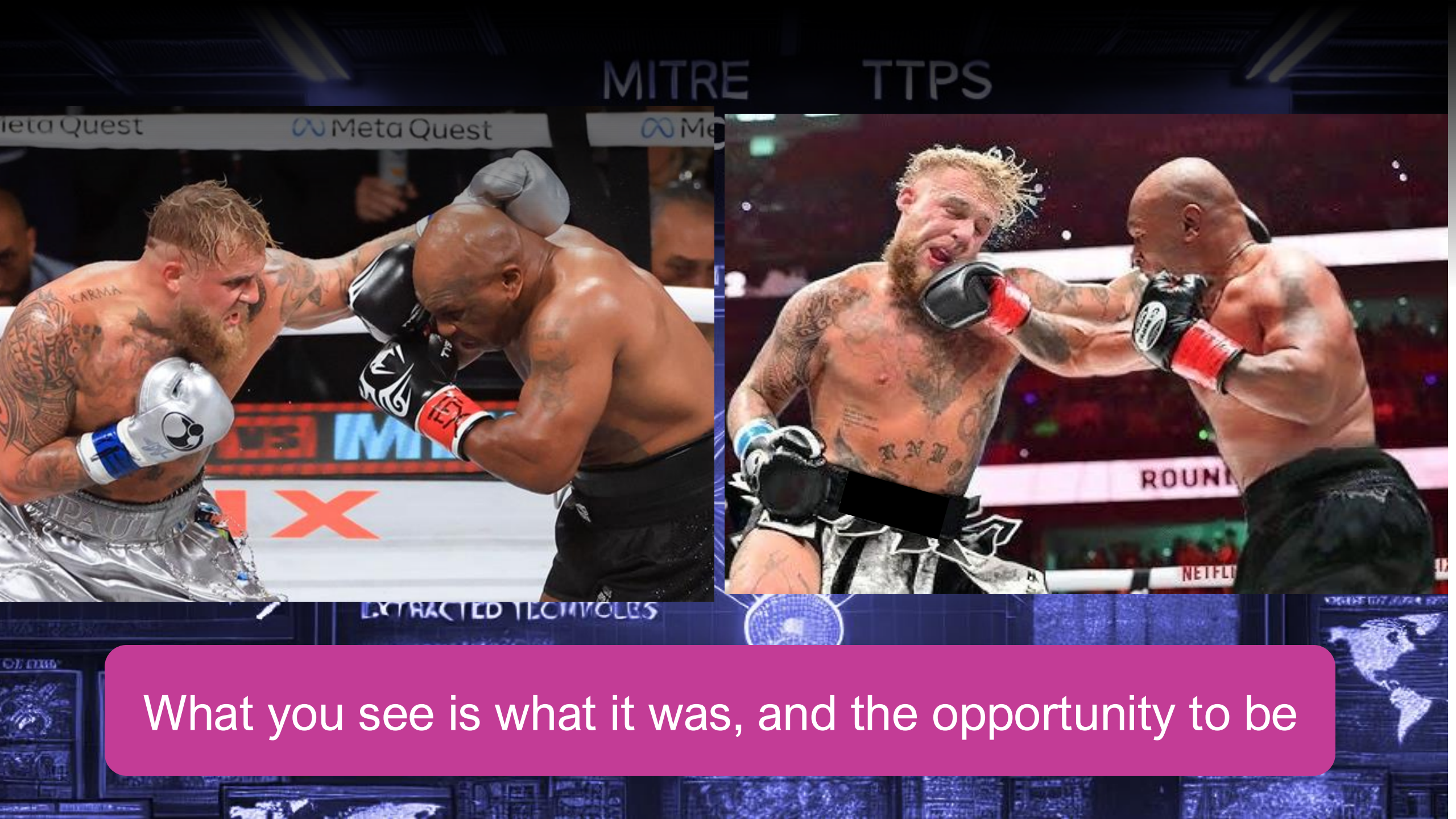
Cross-team feedback

(5 minutes)

RSAC 2025 Conference

Translation of TTPs into activities

“The art of persuasion lies in choosing your words with precision, whether you’re constructing a truth or a lie.”


MITRE
TTPS
Meta Quest
Meta Quest
KARMA
PAUL
ROUNI
NETFLI
What you see is what it was, and the opportunity to be

The vulnerability of the attack

ATT&CK Technique	Adversary Vulnerability	Engagement Activity
When adversaries perform specific actions,	their actions reveal vulnerabilities	that the defender can take advantage of for defensive purposes

ATT&CK Technique	Adversary Vulnerability	Engagement Activity
Remote System Discovery (ATT&CK ID: T1018)	When adversaries interact with the environment or personas, they are vulnerable to collect, observe, or manipulate system artifacts that may cause them to reveal behaviors, use additional or more advanced capabilities against the target, and/or impact their dwell time	Decoy Artifacts and Systems

MITRE | Engage™

"A Practical Guide to Adversary Engagement" (MITRE Engage)

Hitting back - What for?

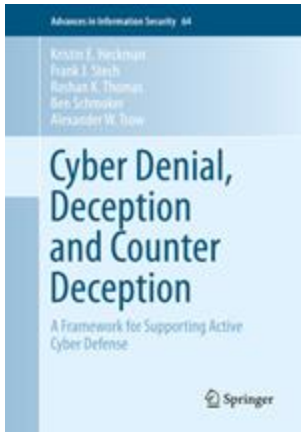
Goal

Rules of engagement

Deception Activity

+Ambiguity
(A-Type)

+Misleading
(M-Type)



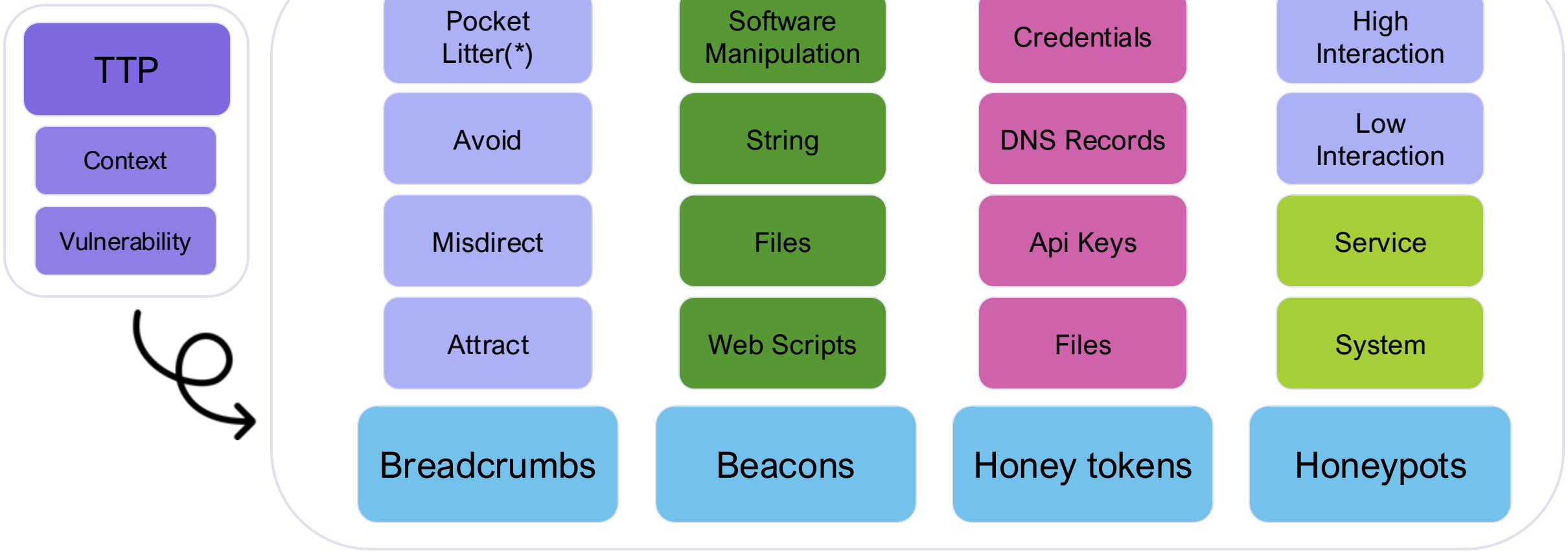
Expose

Affect

Elicit

MITRE | Engage™

Mapping TTPs to Activities



A few tips

Just pick one and try it

- It might be the most used TTP
- Mix creativity with reality
- Start thinking small
- Take care of the risks and the complexity

Defining the activities

(10 minutes)

Cross-team feedback

(5 minutes)

RSAC 2025 Conference

Storytelling Design

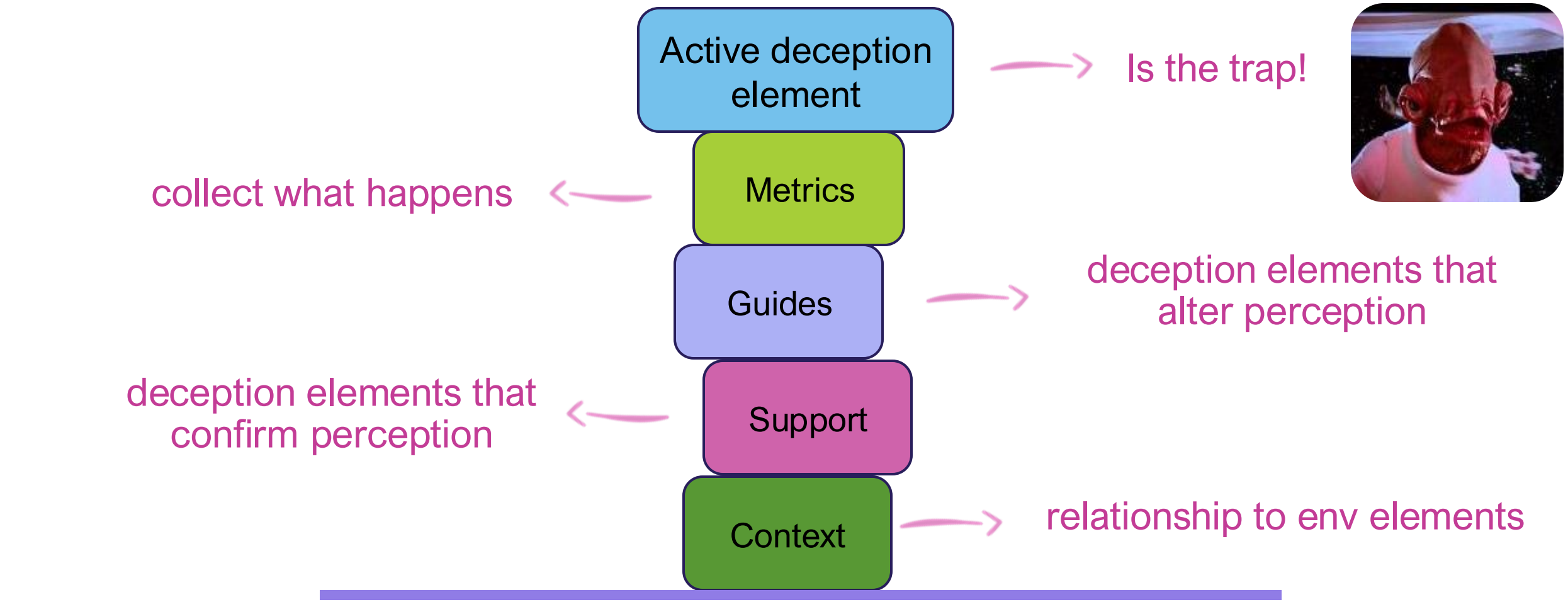
"Every good story begins with a lie that invites us to see the world in a different light."

It's all about the story

- Are there “elements” around our honeypots?
- What role does this “user” have in the organization?
- Is this technology commonly used?
- Why is this service here?

Remember: The narrative supports the whole lie, you are dealing with humans

Elements of a Story



Some examples

A company dedicated to robotics and AI research

- Research notes and pseudo-code snippets in the Dev Team Workstastion that point to a QA web application.
- A DNS record and browser bookmarks for the same web application.

A global financial institution with a trading platform

- Fake user registered on intranet and core services.
- The user is a financial executive with a common name.
- Email credentials “self-leaked".
- The email account is created and registered in some financial social networks.

CYBER-ATTACK
HACKERS
CREATIVE
Tell us a good story
(10 minutes)

Cross-team feedback

(2 minutes)

RSAC 2025 Conference

Many Voices.
One Community.

Questions?

Your next steps

Short term:

- Read your notes and mentally analyze at least five different scenarios for using the deception strategies.

Middle term:

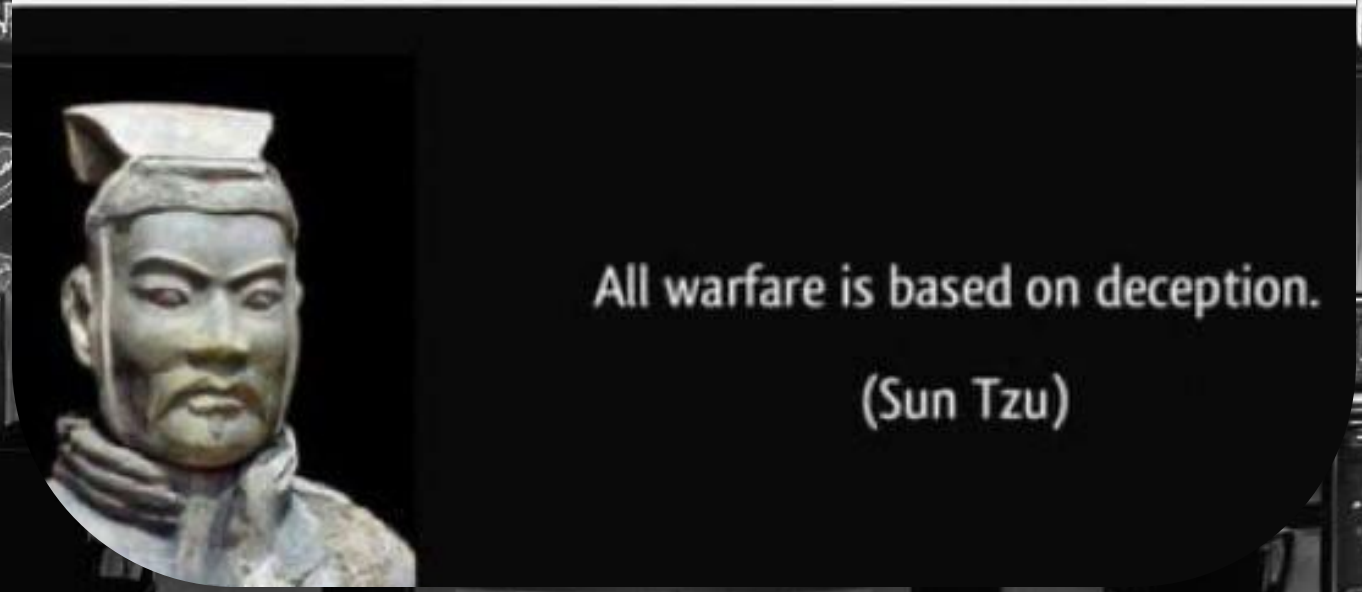
- Try to identify small opportunities to apply deception on your environment (sometimes small is enough).
- Start with zero risk activities.

Long term:

- Define how deception could be part of your detection strategy.
- Deploy in cycles (PLAN - DO - CHECK - ACT).

RSAC 2025 Conference

Many Voices.
One Community.

Thank You

Man Uses an Avocado 'Grenade' & Actually Manages to Rob Two Banks Of RM32,000